

September 11, 2019  
(Via email)

Damon Circosta, Chair  
Stella Anderson  
David C. Black  
Jeff Carmon III  
Kenneth Raymond

North Carolina State Board of Elections  
430 N. Salisbury Street  
Raleigh, North Carolina 27603

Re: Recent Voting System Certifications

Dear Members of the North Carolina State Board of Elections:

We write to urge you to review the governing statutory law concerning state certification of new voting systems and to require full compliance with the scientifically well-grounded election security requirements that North Carolina enacted into law in 2005.

By taking this step long before most national leaders understood the significant vulnerabilities of electronic voting systems and the threats to our nation's election infrastructure, North Carolina established itself as a key national leader on these issues that are critical to our national security and to the State's electoral integrity.

Implementing and complying with the law as written to achieve the General Assembly's objectives to assure accurate, secure elections, will require some time and worthwhile effort when done well. Reliance on the vendors' assurances as to the quality and security of their equipment is not an option that North Carolina law and policy permits.

### **Statutory Charge to the State Board of Elections**

The General Assembly mandated that before the NCSBE certifies a voting system for use within the State, it must conduct a review that includes the source code and "[a]t a minimum"<sup>1</sup> includes review of:

<sup>1</sup> §163A-1115(e) *"Prior to certifying a voting system, the State Board shall review, or designate an independent expert to review, all source code made available by the vendor pursuant to this section and certify only those voting systems compliant with State and federal law. At a minimum, the State Board's review shall include a review of security, application vulnerability, application code, wireless security, security policy and processes, security/privacy program*

- security,
- application vulnerability,
- application code,
- wireless security,
- security policy and processes,
- security/privacy program management,
- technology infrastructure and security controls,
- security organization and governance, and
- operational effectiveness, as applicable to that voting system.

As nationally recognized experts in voting system security and election administration, we commend North Carolina for identifying and requiring analytic attention to this set of points. The provision also authorizes these assessments by retaining an independent expert or an in-house expert qualified to examine source code and other components with regard to the bulleted features.

### **The Current Noncompliance with Statute**

However, it appears based on the information supplied to us, that for the three systems certified on August 23, 2019, the State may have failed to conduct the essential security testing and source code review as part of its certification process. For example, the functional test report delivered by Pro V+V for the ES&S EVS 5.2.2.0 system does not constitute a source code review, nor does it address cybersecurity issues the law specifies. It is our understanding that all recently certified systems had similar Pro V+V reports, but no security or source code review.

The General Assembly's statutory mandate to require an independent review of the voting system source code is a sound practice that more states should employ, following North Carolina's lead.

The EAC testing program for VVSG 1.0, under which the recently certified systems were apparently certified, does not require a detailed source code review

*management, technology infrastructure and security controls, security organization and governance, and operational effectiveness, as applicable to that voting system."*

nor does it emphasize security in the manner in which North Carolina law wisely contemplates.

We urge the State Board to promptly undertake a robust source code review and the required election system security review as required by statute. You may find it helpful to review an example source code review of a voting system from California Secretary of State's "Top to Bottom Review," available at <https://votingsystems.cdn.sos.ca.gov/oversight/ttbr/diebold-source-public-jul29.pdf>

As you undertake the security reviews, we urge the Board to reconsider the use of electronic ballot marking devices such as the ExpressVote as a universal voting device. This new touchscreen voting technology cannot be meaningfully audited and cannot be relied on to produce verifiable results. Such deficiencies could be exposed in the security review. We will write you separately to share some of the scientific findings that explain why such equipment should not be used as standard equipment in public elections.

As members of the scientific community deeply interested in election security, we and our colleagues stand ready to offer our experience and information that may be helpful to you as the Board moves forward to address North Carolina's election security protections. Our professional affiliations are listed below for identification only, as we each sign this letter in our individual capacities.

Respectfully submitted,

Dr. Duncan Buell  
NCR Professor of Computer Science and Engineering  
Dept. of Computer Science and Engineering  
University of South Carolina

Dr. Richard DeMillo  
Charlotte B. and Roger C. Warren Professor of Computing  
Georgia Tech

Dr. Philip B. Stark  
Associate Dean, Division of Mathematical and Physical Sciences

Regional Associate Dean (Interim), College of Chemistry and Division  
of Mathematical and Physical Sciences (ChaMPS)  
Professor, Department of Statistics  
University of California, Berkeley, CA

Harri Hursti  
Security Researcher  
Nordic Innovation Labs  
New York, New York

Dr. Candice Hoke  
Founding Co-Director, Center for Cybersecurity & Privacy Protection C|M Law,  
Cleveland State University

Dr. David Jefferson  
Computer scientist, Lawrence Livermore National Laboratory  
Board of Directors, Verified Voting

Kevin Skoglund  
Chief Technologist  
Citizens for Better Elections, and  
Senior Technical Advisor  
National Election Defense Coalition  
Philadelphia, PA

Susan Greenhalgh  
Vice President of Policy and Programs  
National Election Defense Coalition  
Davis, CA

cc: Karen Brinson Bell  
Katelyn Love